USER INSIGHTS: STRENGTHENING SCAM MITIGATION WITH THE SCAMCLASSIFIER℠ MODEL

The ScamClassifier model was developed by an industry work group to help drive more consistent classification of scams beginning with a common scam definition: ***the use of deception or manipulation intended to achieve financial gain.***

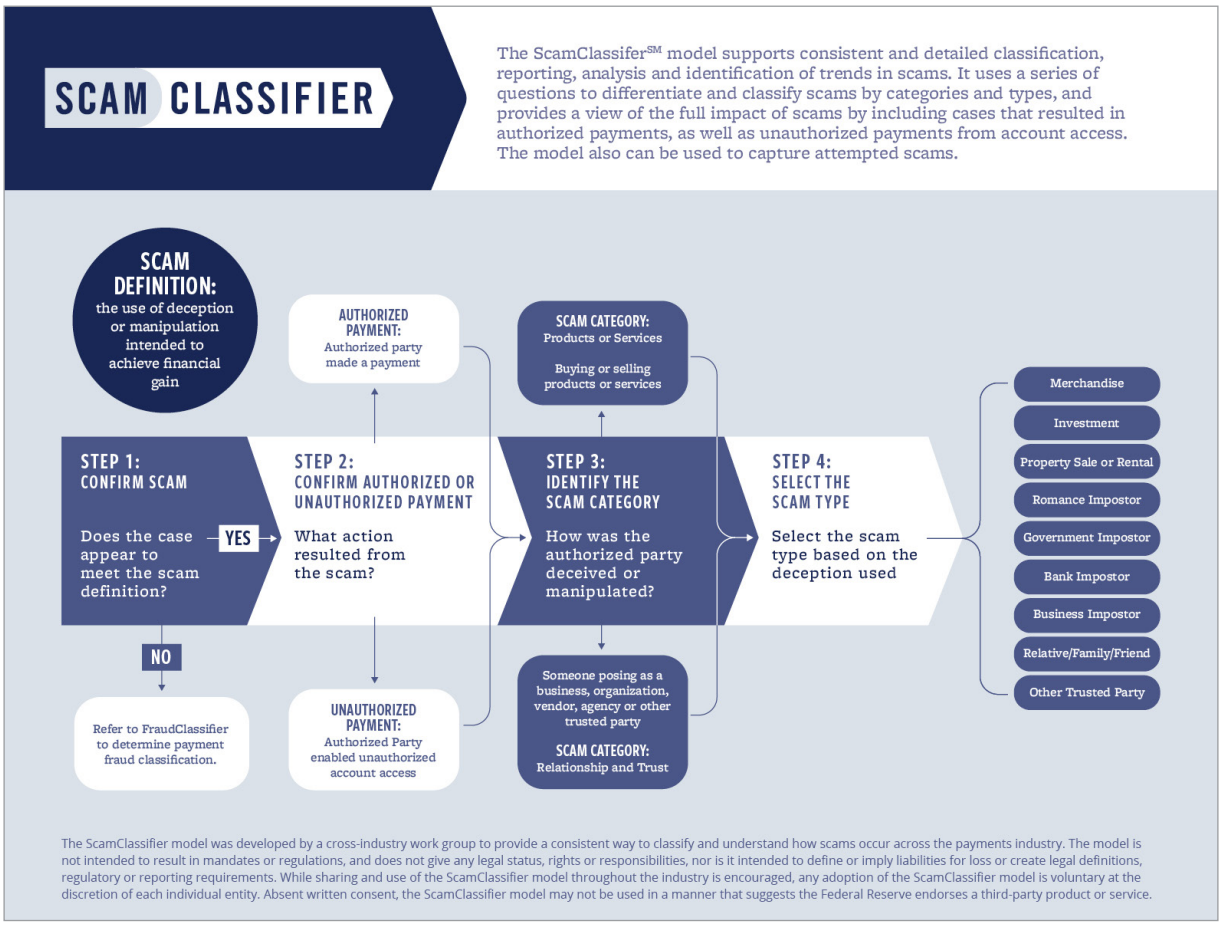
The Federal Reserve checked in with several former work group members for feedback on current and planned uses of the model by their organizations and others. The conversations included potential uses and benefits of the model. Common themes included the value of the model for:

- Targeted prevention and detection
- Streamlined response and resource allocation
- Improved internal education and communication
- Data analysis and trend identification

WHAT IS THE SCAMCLASSIFIER MODEL?

The ScamClassifier model uses a series of questions to differentiate and classify scams by methods, categories and types. Classification begins with the scam definition, **the use of deception or manipulation intended to achieve financial gain**, to distinguish an actual or attempted scam from other types of fraud. Subsequent questions determine the results of the scam, method of deception and type of scam. The model further facilitates accurate scam classification by including definitions and examples of the nine scam types shown in the graphic on the next page.

USER INSIGHTS: STRENGTHENING SCAM MITIGATION WITH THE SCAMCLASSIFIER℠ MODEL



TARGETED PREVENTION AND DETECTION

The ScamClassifier model provides greater consistency in scam type classification for reporting and analytics. This knowledge can be applied to refine payment detection strategies and transaction alerts so organizations can warn their customers about possible payment scams. For example, if a financial institution determines its customers have been sending payments due to merchandise scams, it can more quickly adjust detection strategies to identify payments that fit this scenario. Through more consistent scam reporting, financial institutions may identify merchant names, receiving accounts or other common payment details that can be used in detection. Consistent reporting of scam categories and scam types also is important to facilitate benchmarking performance with other organizations and identifying potential improvements or controls.

USER INSIGHTS: STRENGTHENING SCAM MITIGATION WITH THE SCAMCLASSIFIER℠ MODEL

STREAMLINED RESPONSE AND RESOURCE ALLOCATION

Work group members at some organizations mentioned using the ScamClassifier model to help employees more efficiently respond to scams. This internal training may include how to manage the different results of a scam, such as a completed payment, an attempted scam or payment, or compromised account and login credentials. Financial institutions may choose to route customer reports of scams to designated internal resources. These employees then can initiate claims, document the scam details, take steps to protect their customers' accounts and/or attempt payment recovery. In particular, improved claim intake and internal routing can save time that may be critical to successful payment recovery. Furthermore, directing scam victims to employees trained to respond to scam reports can provide meaningful support for the financial institution's customers. To support employee training on how to identify and handle scams, some organizations have updated their policies and procedures to include the ScamClassifier model.

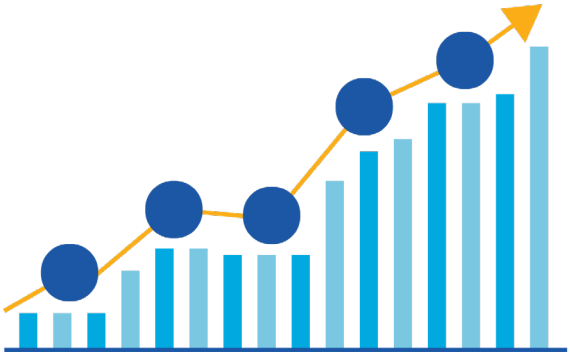
IMPROVED INTERNAL EDUCATION AND COMMUNICATION

The ScamClassifier model and scam definition also can help an organization's employees better recognize a potential scam. Some organizations are using the ScamClassifier model and supporting content in training new employees who are taking on fraud and scam prevention roles, and at an enterprise level in some cases. Customer support employees who gain a more robust understanding of scams may be able to ask customers more discerning questions, listen for red flags, verify the true intent of payments and prevent scams.

To support internal communications within their organizations, employees have access to the same terms and a shared understanding based on the ScamClassifier model. For example, when a teller or customer service representative refers a scam case to their organization's fraud or scams teams, the model's common terminology allows organizations to more effectively document the type of scam and if — and how — a payment occurred.

DATA ANALYSIS AND TREND IDENTIFICATION

Fraud investigators are using the ScamClassifier model for consistency in reporting and to improve their ability to discuss scams internally with internal business partners. They also are communicating with external partners using the model's scam categories and types for more effective discussions about the events and root causes. This consistency helps organizations exchange information and compare their detection rates, losses and other performance metrics with other organizations.



USER INSIGHTS: STRENGTHENING SCAM MITIGATION WITH THE SCAMCLASSIFIER℠ MODEL

Consistent classification of scams supports analytics to identify scam trends that can be used to alert clients about potential risks. For example, a financial institution may see a scam type operating in a specific city or region and notify its customers in that geographic area. As another example, a financial institution that identifies a bank impostor scam reported by multiple customers may be able to notify all its customers about details of the scam approach and help them protect their money by including a reminder to never share account details, online banking credentials or make a potentially suspicious payment to strangers.

LAYING THE GROUNDWORK FOR SCAM PREVENTION

The ScamClassifier model was intended to solve a problem identified by the industry by creating a simple, intuitive tool that can be used across different organizations within the payments industry. Work group members' user insights as described here illustrate the model as a framework for targeted prevention and detection, streamlined response and resource allocation, improved education and communication, and data and trend analysis. The ability to categorize and quantify scams that occur within the payments industry will help organizations further analyze this data to identify the full impact of scams, take steps to mitigate them and better protect their customers.

Learn more and access the ScamClassifier model, including its supporting terms and definitions and examples of classification scenarios.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.